

5

Claims

1. A security module for use with a terminal, comprising

10

a data interface adapted to be coupled to a terminal,
for receiving at least part of an algorithm code or of
the complete algorithm code from the terminal, with the
algorithm code concerning a processing of secrets,

15

an energy interface for receiving supply energy from
the terminal;

20

a volatile memory for storing the part of the algo-
rithm code or the complete algorithm code received via
the data interface, said volatile memory being coupled
to the energy interface in order to have energy sup-
plied thereto such that the same will be cleared upon
an interruption of the receipt of the supply energy
from the terminal; and

25

a processor for performing the algorithm code in order
to obtain an algorithm code result that can be deliv-
ered to the terminal.

30

2. A security module, further comprising:

a non-volatile memory in which the non-received re-
mainder of the algorithm code is stored.

35

3. A security module according to claim 1,
further comprising:

a means for performing an authentication between the
terminal and the security module.

40

5 4. A security module according to any of claim 1,
wherein the data interface is arranged to receive from
the terminal said part of the algorithm code or the
complete algorithm code in encrypted form and/or a cer-
tificate, with the security module further comprising:

10

a means for decrypting said part of the encrypted algo-
rithm code or the encrypted complete algorithm code;
and

15

a means for examining the certificate and for prevent-
ing performing of the algorithm code if said certifi-
cate lacks genuineness.

20

5. A security module according to any of claim 1,
further comprising:

a memory managing unit for controlling memory accesses
of the processor, with the transferred part of the al-
gorithm code containing addresses of the algorithm
code.

25

6. A security module according to any of claim 1,
further comprising:

30

a means for monitoring a predetermined security condi-
tion and for clearing the volatile memory if said pre-
determined security condition is fulfilled, with said
security condition being selected from a plurality of
conditions comprising an interruption, an irregularity
and a fluctuation of the supply voltage and of a system
clock as well as of additional operating parameters.

35

7. A security module according to any of claim 1,
wherein the algorithm code comprises a program code se-
lected for carrying out a task selected from a group
comprising a symmetric cryptographic algorithm, an

40

5 asymmetric cryptographic algorithm, an RSA algorithm, a
cryptographic process according to the DES standard, an
elliptic curve process and an access function for ac-
cessing as well as an access function for changing a
value stored on the security module.

10

8. A security module according to any of claim 1,
wherein the part received of the algorithm code com-
prises a start address of the algorithm code, memory
addresses of computing components necessary for per-
15 forming the algorithm code, or jump addresses of the
algorithm code.

20

9. A security module according to any of claim 1,
wherein the volatile memory is arranged for storing a
newly received, altered part of the algorithm code over
the stored part of the algorithm code or the stored
complete algorithm code.

25

10. A security module according to any of claim 1,
wherein said security module is designed as a chip
card.

30

11. A process for computing an algorithm code result using
a security module, comprising the steps of:

receiving at least part of an algorithm code or the
complete algorithm code by means of an energy inter-
face, with the algorithm code concerning a processing
of secrets;

35

volatile-storing said part of the algorithm code or
said complete algorithm code in a volatile memory of
the security module, with the volatile memory being
coupled to the energy interface, to be supplied with
40 energy, such that the same will be cleared upon an in-

5 interruption of the receipt of the supply energy from the terminal:

performing said algorithm code on the security module in order to obtain an algorithm code result;

10

delivering said algorithm code result to the terminal; and

15

clearing said volatile memory upon an interruption of the receipt of the supply energy from the terminal.

12. A process according to claim 11, wherein said step of clearing comprises removing the security module from the terminal.

20

13. A terminal for use with a security module, comprising:

25

a data interface adapted to be coupled to the security module, for transmitting at least part of an algorithm code or the complete algorithm code from the terminal to a volatile memory of the security module and for receiving the algorithm code result from the security module, with the algorithm code concerning a processing of secrets; and

30

an energy interface for delivering supply energy to the security module, with the volatile memory being supplied by the supply energy, such that the same will be cleared upon an interruption of the receipt of the supply energy from the terminal,

35

with the terminal, for each communication operation between terminal and security module during one and the same communication operation with the security module, being designated to

40

5 send at least the part of the algorithm code or
the complete algorithm code to the volatile mem-
ory of the security module; and,

10 subsequently, during the further communication
process, receive the algorithm code result from
the security module.

14. A process for controlling a security module using a
terminal in order to obtain an algorithm code result
15 from the security module, with the process comprising
for each communication operation, performing the fol-
lowing steps during one and the same communication op-
eration with the security module:

20 delivering supply energy from the terminal to the secu-
rity module;

25 transmitting at least part of an algorithm code or the
complete algorithm code from the terminal to a volatile
memory of the security module, with the algorithm code
concerning a processing of secrets, with the volatile
memory being supplied by the supply energy, such that
the same will be cleared upon an interruption of the
receipt of the supply energy from the terminal; and

30 receiving the algorithm code result from the security
module.

15. A process for communication between a security module
35 and a terminal, comprising the steps of:

40 transferring at least part of an algorithm code or the
complete algorithm code from the terminal to the secu-
rity module, with the algorithm code concerning a proc-
essing of secrets;

5 volatile-storing said part of the algorithm code or
 said complete algorithm code in a volatile memory of
 the security module, with the volatile memory being
 supplied by the supply energy, such that the same will
10 be cleared upon interruption of the receipt of the sup-
 ply energy from the terminal;

 performing said algorithm code on the security module
 in order to obtain an algorithm code result;

15 delivering said algorithm code result to the terminal;
 and

 clearing said volatile memory upon an interruption of
 the receipt of the supply energy from the terminal.

20

16. A process according to claim 15, further comprising:

 repeated transferring of a plurality of different ver-
 sions of said part of the algorithm code or said com-
25 plete algorithm code; and

 storing the repeatedly transferred version of said part
 of the algorithm code or of the complete algorithm code
 over the stored part of the algorithm code or over the
30 complete stored algorithm code.